Cyberpsychology, Behavior, and Social Networking
Volume 27, Number 10, 2024

DOI: 10.1089/cyber.2024.0307

EDITORIAL

Open camera or QR reader and scan code to access this article and other resources online.

Wired for Exhaustion: The Urgent Need for Human-Centric Cybersecurity

Brenda K. Wiederhold, PhD, MBA, BCB, BCN

You get an e-mail from your supervisor. It's brief and direct, typical of her communication style. She's asking you to look at a new report, which is hyperlinked in the body of her e-mail. It's late, and you're tired, so you don't remember all the red flags from the IT team's e-mail safety talk. Your computer hasn't been updated in quite a long time. You haven't set up two-factor authentication on anything because it's inconvenient. You don't verify the sender's e-mail address. You click the link—and reveal the e-mail messages and private information of millions of people.

This scenario is all too common in today's digital landscape, where the convenience of technology often overshadows the critical need for vigilance in cybersecurity practices. The increasing complexity and frequency of cyber threats demand a robust and multifaceted defense strategy. Despite this, the emphasis on technological solutions frequently overshadows an equally crucial aspect: the human element in cybersecurity. Understanding the psychological and behavioral dimensions of how individuals interact with technology can significantly enhance our defenses against cyber threats.

Defending an organization's technical infrastructure is akin to a battleground. There are assailants with nefarious goals and victims caught in the crossfire. Cybersecurity professionals stand on the frontlines overseeing an organization's information, cyber, and technology security. They implement measures to prevent cyberattacks and manage the fallout if system security is compromised. Insights from cyberpsychology, which studies how human behavior interacts with technology, can significantly boost cybersecurity efforts. By understanding how the mind works, organizations can better combat social engineering attacks, phishing, and other mind-manipulation techniques used by cybercriminals.[1]

While cybercriminals seek to exploit technical vulnerabilities, the defenders of our digital frontiers grapple with an unacknowledged adversary: stress, burnout, and fatigue. About 90% of Chief Information Security Officers (CISOs) are overworked and would be willing to take a pay cut if it improved their work-life balance. Additionally, 17% of CISOs use medication or alcohol to cope with stress, 60% rarely unplug from their jobs, and 88% report working more than 40 hours per week.[2] Compared with other high-stress jobs, such as aviation and medicine, the cybersecurity field —and the impact of stress on it—is poorly studied. Yet, overworked and highly fatigued tech professionals can have serious repercussions for individuals, businesses, and industries. It's essential for organizations to consider not just the technological side of their network defenses but also the human side, equipping cybersecurity teams with the support they need to truly thrive.

The Unseen Frontline: The Toll of Constant Vigilance

Cybersecurity operations fundamentally rely on human vigilance, expertise, and resilience. Professionals in the cybersecurity industry must respond to attacks immediately, often working more than 12 hours per day in the first 72 hours of responding to a cyberattack.[3] According to an industry report, 55% of cybersecurity professionals say they experience stress at work half the time, and 28% of CISOs are likely to leave their jobs due to high rates of burnout.[4]

Stress stems from multiple sources, such as the rapid pace of digital transformation, a shortage of qualified staff, operational demands, the need to manage a remote workforce, and chronic cybersecurity threats from malicious cybercriminals and human error (such as employees clicking on a questionable link).[5] These demanding responsibilities can lead to increased stress levels and health concerns ranging from heart disease and sleep problems to depression and substance abuse.[6] Moreover, the burnout and fatigue have ripple effects that impact entire security teams and reduce their capacity to effectively respond to threats. Failing to address these issues leads to upticks in data breaches, cyberattacks, ransomware attacks, and other security concerns.[7]

Psychological Warfare: The Exploitation of Vulnerabilities

Cybercriminals use an array of complicated tactics to infiltrate a company's defenses, ranging from phishing attempts —in which fraudulent e-mails or other messages are sent to a large number of individuals—to targeted attacks that prey on specific employees. For example, a cybercriminal may use public databases and organizational charts to find an employee's phone number, pretend to be their coworker, and ask for sensitive information to gain access to an organization's internal network.

Internal threats also pose significant risks. A Gartner survey conducted in 2022 revealed that 69% of employees bypassed their organization's cybersecurity guidance in the previous year, and 74% of employees said they would be willing to bypass cybersecurity guidance if it helped them or their team achieve a business objective.[8] Additionally, the accelerated adoption of remote workforces—and employees using their own devices to access company servers—creates further challenges for cybersecurity professionals because sensitive data may be retrieved and viewed on systems outside of an organization's control. It just takes one employee to click on a phishing link or download a file infected with malware to cause a serious security threat that impacts an organization's bottom line—while also increasing the workload for CISOs.

In this landscape, technological advancements alone are not enough. Even the most advanced security software struggles with the unknown variables of human error. Therefore, cybercriminals often look to exploit human vulnerabilities rather than challenging technical defenses. Businesses need to support the human element of their security programs as well.[1]

Bridging the Gap: Strategies for Combating Stress and Burnout

Addressing the root causes of stress and burnout demands a multifaceted approach, including the implementation of psychological expertise in cybersecurity defenses, establishing anti-fatiguing programs, and sharing strategies to deal with stress, burnout, and security fatigue. Organizations should partner with experts to assess and address the high-friction areas that impede human performance in cybersecurity, such as operational demands (constant turnover leading to constant on-boarding and off-boarding procedures), and cybersecurity awareness and training for cybersecurity professionals and nontechnical personnel alike. Basic security best practices, such as using two-factor authentication and installing protective software on remote devices, should be required and enforced.

Additionally, establishing and investing in anti-fatiguing programs can help lessen the cognitive load of cybersecurity professionals. Businesses can help reduce or eliminate security fatigue by using AI-driven tools to identify potentially concerning activity, automating any available processes like patches and upgrades, and resourcing cybersecurity teams appropriately. Once these big-pillar moves are made, organizations should share strategies to help employees cope with stress in healthier, more meaningful ways. Integrating cyberpsychology into training programs can enhance these strategies by addressing how employees perceive and respond to cyber threats.[1]For example, stress inoculation training (SIT) uses several phases to create a comprehensive and preventative approach to stress management, beginning with an awareness of how stress manifests in the body, the implementation of coping mechanisms like relaxation exercises or cognitive strategies to reframe negative thoughts, and the application of these techniques in real-life scenarios.[9]

SIT can be paired with other approaches designed to help people learn how to manage their fight-or-flight response in the face of stressors. Research suggests that virtual reality therapy can help people learn how to use those coping strategies in simulated environments—a practice that has found success in populations ranging from military personnel to medical staff.[10,11] Where possible, organizations should offer stress management services to employees and encourage their use, giving cybersecurity professionals the tools they need to manage a barrage of cyberattacks with a sense of resiliency.

These solutions should happen in tandem; mindfulness strategies may help an overworked employee, but a business must also address the systemic issues that contribute to cybersecurity fatigue. All the coping strategies in the world will not solve a chronically under-resourced cybersecurity team. The pursuit of cyber defense, while indispensable, should not come at the cost of the defenders' well-being. As the digital battlefield evolves, so too must our strategies for supporting the human element within cybersecurity, ensuring these professionals can continue to protect our digital lives without sacrificing their own mental and physical health.

Brenda K. Wiederhold
Editor-in-Chief

References

1. Pratt M. (2023). Why Cyberpsychology is Such an Important Part of Effective Cybersecurity. CSO Online Available from: https://www.csoonline.com/article/643967/why-cyberpsychology-is-such-an-important-part-of-effective-cybersecurity.html [Last accessed: April 2, 2024].
2. The CISO Stress Report – Life Inside the Perimeter: One Year On. (2020) Nominet. Available from: https://www.nominet.uk/nominet-ciso-stress-report-one-year-on/ [Last accessed: April 2, 2024].
3. Singh T, Johnston AC, D'Arcy J, et al. Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. OCJ 2023;3(2): 100–126.
4. The Life and Times of Cybersecurity Professionals. (Volume 6). (2023). ISSA Available from: https://www.issa.org/new-research-from-techtargets-enterprise-strategy-group-and-the-issa-reveals-continuous-struggles-within-cybersecurity-professional-workforce/ [Last accessed: April 4, 2024].
5. Nobles C. Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA–Journal of Business and Public Administration 2022;13(1):49–72; doi: 10.2478/hjbpa-2022-0003
6. Valcour M. (2016). Beating burnout. Harvard Business Review, *94*(11), 98–101. Available from: https://www.researchgate.net/profile/Monique-Valcour/publication/308986353_Beating_Burnout/links/57fcd87b08ae4189fee40aaf/Beating-Burnout.pdf [Last accessed: April 4, 2024].
7. Nobles C. Establishing human factors programs to mitigate blind spots in cybersecurity. MWAIS 2019 Proceedings 2019;22https://aisel.aisnet.org/mwais2019/22. [Last accessed: April 2, 2024].
8. Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025. (2023). Gartner Available from: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025 [Last accessed: April 3, 2023].
9. A new reality: SBIR solution builds warfighter resiliency before, during, and after combat tours. (2022). Department

of Defense Small Business Innovation Research Available from: https://vrphobia.com/wp-content/uploads/2023/05/VRMC_STORY.pdf [Last accessed: April 2, 2024].
10. Wiederhold BK, Bouchard S, Wiederhold BK, et al. (2014). Virtual reality for posttraumatic stress disorder. *Advances in virtual reality and anxiety disorders*, 211–233. Available from: https://link.springer.com/chapter/10.1007/978-1-4899-8023-6_10 [Last accessed: April 4, 2024].
11. Wiederhold BK. The stress vaccine? How technology can increase resilience. Cyberpsychol Behav Soc Netw 2024; 27(4):235–237.